



CAPITOL

Technology University

October 16, 2023

Dr. Sanjay Rai
Secretary of Maryland Higher Education
Maryland Higher Education Commission
6 N. Liberty Street
Baltimore, MD 21201

Dear Dr. Rai,

Capitol Technology University is requesting approval to offer a Bachelor of Science in **Cybersecurity** program on the Notre Dame of Maryland University (NDMU) campus in Towson, Maryland while NDMU will offer a **Bachelor of Arts in Leadership in Hospitality and Event Management** program on the CTU Laurel campus. The degree curriculum will be taught using a significant number of existing faculty at our university and will be supplemented by new courses supporting the **BS in Cybersecurity**. The mission of Capitol Technology University is to provide practical education in engineering, computer science, information technology, and business that prepares individuals for professional careers and affords the opportunity to thrive in a dynamic world. A central focus of the university's mission is to advance practical working knowledge in areas of interest to students and prospective employers within the context of Capitol's degree programs. The university believes that offering a **BS in Cybersecurity** on the Notre Dame of Maryland University (NDMU) campus is consistent with this mission.

Educational and professional organizations are reporting significant workforce shortages of trained personnel in the field of Cybersecurity. Moreover, the shortage is growing each year with increasing demand to replace cybersecurity professionals who are reaching retirement age. This program is in response to help meet that need. The **BS in Cybersecurity** degree has been the most popular undergraduate program at Capitol for nearly 10 years. The opportunity to reach a larger audience of Maryland students by offering our successful Cybersecurity program at the Notre Dame of Maryland campus, Capitol Technology University will be able to expand its reach to ensure that Maryland meets the growing demands for cyber professionals in the private, public, and government sectors.

To respond to the growing need for cybersecurity professionals, we respectfully request approval offer the **BS in Cybersecurity** on the Notre Dame of Maryland University (NDMU) campus. The required proposal is attached as well as the letter from me as university president confirming the adequacy of the university's library to serve the needs of the students in this degree.

Respectfully,

Bradford L. Sims, PhD
President



CAPITOL
Technology University

October 16, 2023

Dr. Sanjay Rai
Secretary of Maryland Higher Education
Maryland Higher Education Commission
6 N. Liberty Street
Baltimore, MD 21201

Dear Dr. Rai,

This letter is in response to the need for confirmation of the adequacy of the library of Capitol Technology University to support offering **BS in Cybersecurity** on the Notre Dame of Maryland University (NDMU) campus through our extensive virtual library. As president of the university, I confirm that the library resources, including support staff, are more than adequate to support the **BS in Cybersecurity**. In addition, the university is dedicated to, and has budgeted for, continuous improvement of its library resources.

Respectfully,

Bradford L. Sims, PhD
President



Cover Sheet for In-State Institutions

New Program or Substantial Modification to Existing Program

Institution Submitting Proposal

Capitol Technology University

Each action below requires a separate proposal and cover sheet.

- | | |
|---|---|
| <input type="radio"/> New Academic Program | <input type="radio"/> Substantial Change to a Degree Program |
| <input type="radio"/> New Area of Concentration | <input type="radio"/> Substantial Change to an Area of Concentration |
| <input type="radio"/> New Degree Level Approval | <input type="radio"/> Substantial Change to a Certificate Program |
| <input type="radio"/> New Stand-Alone Certificate | <input type="radio"/> Cooperative Degree Program |
| <input checked="" type="radio"/> Off Campus Program | <input type="radio"/> Offer Program at Regional Higher Education Center |

Payment <input checked="" type="radio"/> Yes	Payment <input type="radio"/> R*STARS # 95609	Payment \$850	Date 10/16/23
Submitted: <input type="radio"/> No	Type: <input type="radio"/> Check # 95609	Amount:	Submitted:

Department Proposing Program	Cybersecurity		
Degree Level and Degree Type	Bachelor of Science (B.S.)		
Title of Proposed Program	Bachelor of Science in Cybersecurity		
Total Number of Credits	120		
Suggested Codes	HEGIS: 70116.00	CIP: 111003.0000	
Program Modality	<input checked="" type="radio"/> On-campus <input type="radio"/> Distance Education (fully online) <input type="radio"/> Both		
Program Resources	<input checked="" type="radio"/> Using Existing Resources <input type="radio"/> Requiring New Resources		
Projected Implementation Date <small>(must be 60 days from proposal submission as per COMAR 13B.02.03.03)</small>	<input checked="" type="radio"/> Fall <input type="radio"/> Spring <input type="radio"/> Summer Year: 2024		
Provide Link to Most Recent Academic Catalog	URL: https://catalog.captechu.edu		

Preferred Contact for this Proposal	Name:	Allen Exner
	Title:	Director of Library Services and Information Literacy
	Phone:	(240) 965-2470
	Email:	ahexner@captechu.edu

President/Chief Executive	Type Name:	Dr. Bradford L. Sims
	Signature:	Date: 10/16/2023
		Date of Approval/Endorsement by Governing Board: 10/16/2023

PROPOSAL FOR:

____ NEW INSTRUCTIONAL PROGRAM
X SUBSTANTIAL EXPANSION/MAJOR MODIFICATION
____ COOPERATIVE DEGREE PROGRAM
____ WITHIN EXISTING RESOURCES or ____ REQUIRING NEW RESOURCES



CAPITOL
Technology University

Institution Submitting Proposal

Fall 2024
Projected Implementation Date

**Bachelor of Science
(B.S.)**
Award to be Offered

70116
Suggested H.E.G.I.S. Code

Cybersecurity
Department of Proposed Program

Dr. Kellep Charles
Department Chair

kacharles@captechu.edu
Contact E-Mail Address

**Bachelor of Science in
Cybersecurity**
Title of Proposed Program

111003
Suggested C.I.P. Code

Dr. Kellep Charles
Name of Department Head

301-369-3609
Contact Phone Number

 **10-16-23**
Signature and Date

President/Chief Executive Approval

OCT. 16, 2023
Date

Date Endorsed/Approved by Governing Board

**Proposed Bachelor of Science in Cybersecurity
Department of Department of Cybersecurity
Capitol Technology University
Laurel, Maryland**

A. Centrality to Institutional Mission and Planning Priorities:

- 1. Provide a description of the program, including each area of concentration (if applicable), and how it relates to the institution's approved mission.**

Bachelor of Science in Cybersecurity Program Description:

The Bachelor of Science in Cybersecurity degree is a unique program designed to meet the emerging needs of today's economy, which is experiencing significant labor gaps in critical cyber professions. Capitol Technology Cybersecurity program has been producing graduates that are prepared for the workforce since 2000 but according to current employment trends there is still a significant shortage of cybersecurity workers to fill the current positions. Therefore, Capitol Technology University (CTU) proposes to offer a Cybersecurity program on the Notre Dame of Maryland University (NDMU) campus in Towson, Maryland while NDMU will offer a Bachelor of Arts in Leadership in Hospitality and Event Management program on the CTU Laurel campus. This partnership will provide students within the Baltimore and surroundings area the opportunity to enroll in a Cybersecurity program that has connections with various security agencies and offers students within the surrounding Laurel area access to a Hospitality and Event Management program that provides a more interactive learning environment.

Capitol Technology University Cybersecurity program prepares students with the skills needed for entry level positions that defend the nation's critical infrastructure from cybercriminals. Cybersecurity skills in which there are currently significant shortage to fill the numerous vacancies available throughout the United States. According to the latest International Information System Security Certification Consortium (ISC)² 2022 Cybersecurity Workforce Study this cybersecurity workforce gap threatens the most foundational functions of the profession, such as risk assessment, oversight and critical systems patching, according to the study. More than half of employees at organizations with workforce shortages feel that staff deficits put their organization at an "moderate" or "extreme" risk of cyberattacks. In addition, that risk increases substantially when organizations have a significant staffing shortage (ISC², 2022). A 2016 Center for Strategic and International Studies (CSIS) survey of I.T. decision-makers across eight countries found that 82 percent of employers report a shortage of cybersecurity skills, and 71% believe this talent gap causes direct and measurable damage to their organizations. According to Cyberseek, funded by the National Initiative for Cybersecurity Education (NICE), there are currently over 600,000 cybersecurity positions currently available in the United States and 30% of those positions within the DC/MD/VA area.

Within, the Baltimore/Towson/Columbia area there are over 15,000 vacant cybersecurity positions that are currently open. The Cybersecurity program on the NDMU campus will be tremendous force in graduating students with the skills they need to enter the workforce. The Bachelor of Science in Cybersecurity program introduces students to the basic concepts of securing data, data integrity and confidentiality. The program challenges students to become proficient in risk management, virtualization, vulnerability scanning and mitigation. Upon completion of the program students will have mastered skills in cryptography, digital forensics, malware analysis and penetration testing. Throughout

their undergraduate career students will have access to Faculty who are currently employed within cybersecurity agencies that are focused on developing and implementing cutting edge techniques to thwart the ever-evolving cyber threats.

The Cybersecurity program at Capitol Technology University emphasizes hands-on learning and students will have the opportunity to work in the Security Operations center where they learn incident handling, log analysis and basic analytics. This is a the common practice at the Laurel campus and we plan to also have a cyber security lab on the NDMU campus. In addition to their laboratory participation students have the opportunity to develop and hone their skills in cyber competitions. All of these experiences and skills will equip students to pursue a career in cyber security but before they do that, they have an array of opportunities to obtain internships that challenges their knowledge and skills even further.

The Bachelor of Science in Cybersecurity program is accredited by the Accreditation Board for Engineering and Technology (ABET) and is designated as a NSA Center of Excellence in Cyber Defense Education (CAE-CDE). It is one of the few programs in the nation that have the honor of receiving both of these designations.

CSIS, *Hacking the Skills Shortage* (Santa Clara, CA: McAfee, July 2016), <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf>.
CyberSeek, "Cybersecurity Supply/Demand Heat Map," accessed October 3, 2023, <https://www.cyberseek.org/heatmap.html>.

2. Explain how the proposed program supports the institution's strategic goals and provide evidence that affirms it is an institutional priority.

Capitol Technology University operates on four strategic goals:

- 1. Expand Educational Offerings, Increase Program Completion:** *Capitol Technology University is an institution that offers career-relevant curricula with quality learning outcomes. The strategy includes continuing to expand educational offerings, increasing program completion, and raising learner qualifications and outcomes.*
- 2. Increase Enrollment and Institutional Awareness:** *Capitol will accelerate its goal to become more globally renowned and locally active through student, faculty and staff activities. Enrollment will grow to 650 undergraduates, 350 masters' students and 350 doctoral candidates.*
- 3. Improve the Utilization of University Resources and Institutional Effectiveness While Expanding Revenue:** *Capitol will likely continue to be 80% financially dependent on student tuition and fees. We plan to enhance our resources by expanding the range and amount of funding from other streams and aligning costs with strategic initiatives.*
- 4. Increase the Number and Scope of Partnerships:** *Capitol's service to our constituents and sources of financial viability both depend upon participation with continuing and new partner corporations, agencies, and schools.*

The Bachelor of Science in Cybersecurity program supports all the University's four strategic goals. The proposed degree builds upon the existing areas of degrees at the undergraduate level: B.S. in Astronautical Engineering, B.S. in Aviation Professional Pilot, B.S. in Computer Engineering, B.S. in

Computer Engineering Technology, B.S. in Computer Science, B.S. in Construction Information Technology and Cybersecurity, B.S. in Construction Management and Critical Infrastructure, B.S. in Construction Safety B.S. in Cyber Analytics, B.S. in Cybersecurity, B.S. in Data Science, B.S. in Electrical Engineering, B.S. in Electrical Engineering Technology, B.S. in Engineering Technology, B.S. in Facilities Management and Critical Infrastructure, B.S. in Information Technology, B.S. in Management of Cyber and Information Technology, B.S. in Mechatronics Engineering, B.S. in Mechatronics and Robotics Engineering Technology, B.S. in Software Engineering, and B.S. in Technology and Business Management, B.S. in Unmanned and Autonomous Systems, and B.S. in Web Development.

The University's programs have been preparing students for the rapid advances in information technology, intense global competition, and increasingly sophisticated technological environments for decades. This partnership compliments these offerings and provides links with the local and national cyber based employers that offers employers in these field.

The proposed partnership with NDMU is fully supported by the University's 2025 Vision and the FY2017-2025 Strategic Plan. Funding to support the Bachelor of Science in Cybersecurity on the NDMU campus is already available within the existing budget.

The University has active partnerships in the private and public areas (e.g., NASA, Parson Corporation, Leidos, Patton Electronics, Lockheed Martin, Northrup Grumman, Cyber Security Forum Initiative, Internal Revenue Service, and National Cryptologic School). The Bachelor of Science in Cybersecurity degree will provide new opportunities for partnerships. The increase in alliances and the placement of our graduates in our partner institutions will serve to expand the University's enrollment and reputation.

3. Provide a brief narrative of how the proposed program will be adequately funded for at least the first five years of program implementation. (Additional related information is required in section L.)

Capitol Technology University will support the proposed partnership through the same process and level of support as the University's existing programs. The University has also budgeted funds to support program and course development, online support, office materials, travel, professional development, and initial marketing. There is no substantial impact to the institution due to the advanced budgeting of these funds. If approved, the program will be self-sustaining going forward.

4. Provide a description of the institution's commitment to:

a. Ongoing administrative, financial, and technical support of the proposed program

The proposed partnership is an integral part of the University's Strategic Plan for FY 2017-2025 and forward. The institutional and departmental budgets for FY 2022-2023, as well as the forecasted budgets going forward, include funding for the administrative, financial, and technical support of the new partnership.

b. Continuation of the program for a period of time sufficient to allow enrolled students to complete the program.

Capitol Technology University is fully committed to continuing the proposed Bachelor of Science in Cybersecurity degree program on the NDMU campus for a sufficient period to allow enrolled students to complete the program.

B. Critical and Compelling Regional or Statewide Need as Identified in the State Plan:

1. Demonstrate demand and need for the program in terms of meeting present and future needs of the region and the State in general based on one or more of the following:

a. The need for advancement and evolution of knowledge.

The Cyber industry relies on technology, people, and processes as the critical elements required to maintain and grow the industry. This degree matches those critical components by providing relevant knowledge and skills that are implemented in a hands-on learning environment.

b. Societal needs, including expanding educational opportunities and choices for minorities and educationally disadvantaged students at institutions of higher education.

Capitol Technology University is a diverse multiethnic and multiracial institution with a long history of serving minority populations. The University has a 51% minority student population, with 7% undisclosed. The Black/African American population is 34%. The University has a military/veteran population of 22%. The University also has a 22% female population – a significant percentage given its status as a technology institution. The partnership with NDMU which recently became Co-ed in which 96% of students are female, would provide the opportunity to increase the representation of females within the cybersecurity field. In addition, 52% of NDMU student body are members of a minority group. This partnership would provide the ideal grounds for providing educationally disadvantaged students with a campus location that is easily accessible and supports their goals of becoming a cybersecurity professional.

c. The need to strengthen and expand the capacity of historically black institutions to provide high quality and unique educational programs.

While Capitol Technology University is not a historically black institution, the University is a diverse multiethnic and multiracial institution with a long history of serving minority populations. The University has a 51% minority student population, with 7% undisclosed. The Black/African American population is 34%. The University has a military/veteran population of 22%. The University also has a 21% female population – a significant percentage given its status as a technology institution. If approved, the proposed Bachelor of Science in Cybersecurity will expand the field of opportunities for minorities and disadvantaged students. Given the substantial minority population of Capitol Technology University, it is also reasonable to assert that the Bachelor of Science in Cybersecurity program will add to the base of minority participation.

2. Provide evidence that the perceived need is consistent with the Maryland State Plan for Postsecondary Education.

The 2021-2025 Maryland State Plan for Higher Education articulates three goals for postsecondary education:

1. Access
2. Success
3. Innovation

Goal 1: Access

"Ensure equitable access to affordable and quality postsecondary education for all Maryland residents."

Capitol Technology University is committed to ensuring equitable access to affordable post-secondary education for all Maryland residents. The University meets its commitment in this arena through its diverse campus environment, admissions policies, and academic rigor.

The Capitol Technology University community is committed to creating and maintaining a mutually respectful environment that recognizes and celebrates diversity among all students, faculty, and staff. The University values human differences as an asset and works to sustain a culture that reflects the interests, contributions, and perspectives of members of diverse groups. The University delivers educational programming to meet the needs of diverse audiences. We also seek to instill those values, understanding, and skills to encourage leadership and service in a global multicultural society.

The composition of the University's student body reflects the institution's commitment to diversity. Capitol Technology University has a 51% minority student population, with 7% undisclosed. The Black/African American population is 34%. The University has a military/veteran population of 22%. The University also has a 22% female population – a significant percentage given its status as a technology university.

Achievement gaps: The University provides leveling courses in support of individuals attempting a career change to a field of study not necessarily consistent with their current skills. There are situations where undergraduate courses best serve student needs in subject areas. The University makes those courses available.

The University engages in diversity training for its institutional population, including students. Diversity and inclusiveness are built into the curriculum allowing graduates to operate effectively in a global environment. The University supports multiple diversity enhancing actions, including team projects and grants across degrees. This has proven effective at supporting numerous aspects of diversity.

Capitol Technology University does not discriminate on the basis of race, color, national origin, sex, age, sexual orientation, or handicap in admission, employment, programs, or activities.

Through its academic programs, Capitol Technology University seeks to prepare all of its graduates to demonstrate four primary characteristics:

- **Employability:** The ability to enter and advance in technical and managerial careers, appropriate to their level and area of study, immediately upon graduation.
- **Communications:** Mastery of traditional and technological techniques of communicating ideas effectively and persuasively.

- **Preparation of the Mind:** The broad intellectual grounding in technical and general subjects required to embrace future technical and managerial opportunities with success.
- **Professionalism:** Commitment to life-long learning, ethical practice, and participation in professions and communities.

The proposed Bachelor of Science in Cybersecurity program at NDMU and University financial aid will be available to all Maryland residents who qualify academically for admission. The University has successfully managed to support Financial Aid for its students since its founding in 1927.

The Bachelor of Science in Cybersecurity program, with its academic rigor, will produce highly qualified entry level cybersecurity professionals with the highest level of skills and abilities to advance their careers. The University has a proven record of rigorous high-quality education in all of its degrees. The University receives its regional accreditation from the Middle States Commission on Higher Education (MSCHE) and has specialized accreditation from the Accreditation Board for Engineering and Technology (ABET), National Security Agency (NSA), and Department of Homeland Security (DHS) National Centers of Academic Excellence in Cyber Defense Education (NCAE-CDE). The Bachelor of Science in Cybersecurity program is consistent with the MSCHE criteria for regional accreditation of the delivery of high-quality higher education. The NCAE-CDE stated objective addressing the Cyber labor and skills shortfall is also addressed by this proposed degree program.

Goal 2: Success

"Promote and implement practices and policies that will ensure student success."

The courses for the Bachelor of Science in Cybersecurity degree will be offered online using the Canvas Learning Management System and Zoom. The University provides a tuition structure that is competitive with its competitors. The University tuition structure does not differentiate between in-state and out-of-state students. The University's Student Services provide advising, tutoring, virtual job fair attendance, and other activities supporting student completion and employment for both on-ground and online students.

Students receive information throughout the admissions process regarding the cost to attend the University. The information is also publicly available on the University website. The University's Admissions Office and Office of Financial Aid identify potential grants and scholarships for each student. The Office of Financial Aid also provides plans for each student to reduce potential student debt. The net cost versus gross costs is identified clearly for the student. Students receive advising from Financial Aid Advisors before enrolling in classes for the first time. Admissions personnel, Student Services Counselors, and Departmental Chairs advise students of the need for academic readiness as well as the degree requirements. Academic Advisors also develop a specific success pathway for each student.

The University's tuition increases have not exceeded 3%. The University also has a tuition guarantee for undergraduates, which means full-time tuition is guaranteed not to increase more than 1% per year above the rate at the time of initial enrollment. The tuition remains at this rate if the student remains enrolled full-time without a break in attendance.

The University provides services and learning tools to guide students to successful degree completion. Programs such as Early Alert give the University's faculty and staff opportunities for

early student intervention on the pathway to graduation. This program applies to all students regardless of the mode of course delivery or degree program. Capitol Technology University is also a transfer-friendly institution and participates in multiple programs for government and military credit transfer. Capitol Technology University participates in the Articulation System for Maryland Colleges and Universities (ARTSYS) and has numerous transfer agreements with local institutions at all degree levels.

The University has in place services, tutoring, and other tools to help ensure student graduation and successful job placement. The University hosts a career (job) fair twice a year. The University has an online career center available to all students covering such topics as career exploration, resume writing, job search techniques, social media management, mock interviews, and assistance interpreting job descriptions, offers, and employment packages.

The University also works with its advisory boards, alumni, partners, and Faculty to help ensure the degrees offered at the University are compatible with long-term career opportunities in support of the state's knowledge-based economy.

Goal 3: Innovation

"Foster innovation in all aspects of Maryland higher education to improve access and student success."

Capitol Technology University's past, present, and future are inextricably intertwined with innovation. The University has a long tradition of serving as a platform for the use of new and transformative approaches to delivering higher education. New technology and cutting-edge techniques are blended with proven strategies to enable student success in all classroom modalities as well as in a successful career after graduation. As a small institution, Capitol Technology University has the agility to rapidly integrate new technologies into the curriculum to better prepare students for the work environment. The University designs curriculum in alliance with its accreditation and regulating organizations and agencies.

The University also employs online virtual simulations in a game-like environment to teach the application of knowledge in a practical hands-on manner. The University engages with a partner creating high-level virtual reality environments for use by students pursuing this degree. This use of current technology occurs in parallel with traditional, proven learning strategies. These elements of the University's online learning environment are purposeful and intended to improve the learning environment for both the student and faculty member. The approach is intentionally designed to increase engagement, improve outcomes, and improve retention and graduation rates. The University believes that innovation is the key to successful student and faculty engagement.

Example: The University engages its students in fusion projects that allow students to contribute their skills in interdisciplinary projects such as those in our Astronautical Engineering and Cyber Labs. In those labs, students become designers, builders, and project managers (e.g., to send a CubeSat on a NASA rocket) and data analysts (e.g., to analyze rainforest data for NASA). The University's students recently launched their latest satellite aboard a NASA rocket from Norway at the beginning of the 2019 Fall Semester. Students enrolled in the proposed Bachelor of Science in Cybersecurity will be challenged to design, deliver and assess cyber curriculum in a classroom setting under experienced University STEM educators.

C. Quantifiable and Reliable Evidence and Documentation of Market Supply and Demand in the Region and State:

1. Describe potential industry or industries, employment opportunities, and expected level of entry (ex: *mid-level management*) for graduates of the proposed program.

The Department of Commerce National Initiative for Cybersecurity Careers and Studies (NICCS) Workforce Framework for Cybersecurity (NICE Framework) has defined five work roles for the U.S. Government appropriate for this degree program (<https://niccs.cisa.gov/workforce-development/nice-framework>). The prospective students will enter a field that is in high demand and provides numerous areas of focus. Graduates will be able to obtain an entry level position within information assurance or technical areas (Figure 1) in commercial companies as well as local, state, and federal government with a variety of titles such as:

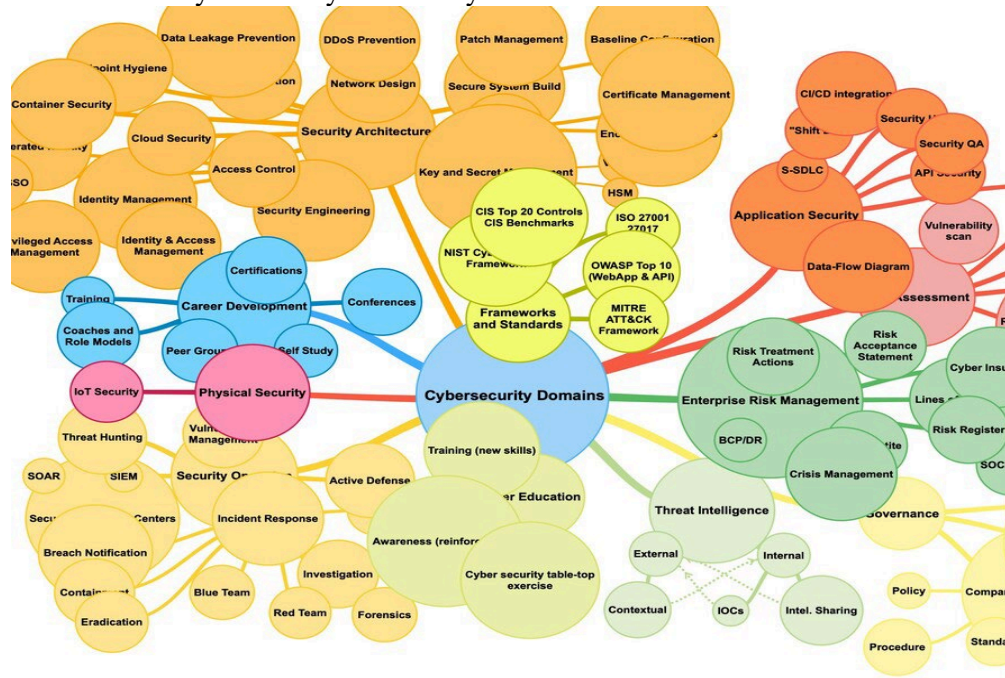
- Cybersecurity Specialist
- Cyber Crime Analyst
- Incident and Intrusion Analyst
- IT Auditor
- Security Intelligence
- Cybersecurity Analyst
- Penetration and Vulnerability Tester
- I.T. Support
- Systems Engineering

Figure 1: Type of positions for cybersecurity personnel

Management	Information Assurance	Technical
<ul style="list-style-type: none">• Cybersecurity Strategy• Legal and Regulatory• Cybersecurity business case formulation• IT Base skills• Staff Management skills/ Leadership skills• Personnel Security• Multi-Disciplinary skills (technology, people etc)• Communication skills• Cyber-Criminal Psychology• Cyber-Ethics Skills	<ul style="list-style-type: none">• Cybersecurity Policies, Standards and Procedures• Risk Management• System Accreditation• Compliance Checking• Audit and Monitoring• User Rights and Responsibilities• Incident Management Process Design• Assurance, trust and confidence mechanisms	<ul style="list-style-type: none">• IT technical skills (security management)• IT technical skills (Security deployment)• Security Design Principles e.g. zoning• Resilient Infrastructure• Data Protection/ System administration• Cryptographic and Applied Crypto Skills• Data custodianship• Operational Security• Incident Management

Consistent with our current graduates, graduates from the NDMU partnership will possess the skills needed to obtain entry-level cyber security positions (Figure 2).

Figure 2: Topic areas where Cybersecurity is currently established.

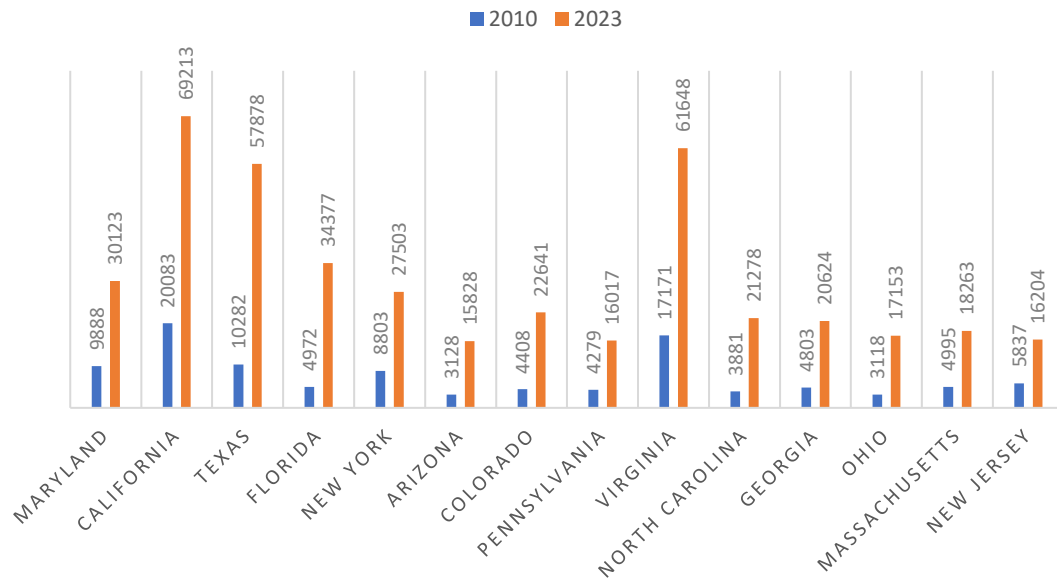


2. Present data and analysis projecting market demand and the availability of openings in a job market to be served by the new program.

According to Cyberseek, there are currently 663, 434 cybersecurity positions available in the U.S., which is a 77% increase from 2010. On a national scale, there are only enough cybersecurity workers to fill 69% of the cybersecurity positions. The demand for cybersecurity positions within the state of Maryland is 68% which is similar to the national numbers. This is a 67% increase in the number of available cybersecurity positions from 2010 which is trend that is being experienced nationwide. The need for trained cybersecurity is even more evident with research indicating that the industry is expected to grow by 11% in 2023 and 20% in 2025 (Figures 3 & 4). With only 400,000 cybersecurity professionals being trained by 2023 the need for institutions of higher education to offer this program to more students is necessary for the nation to meet the needs of society.

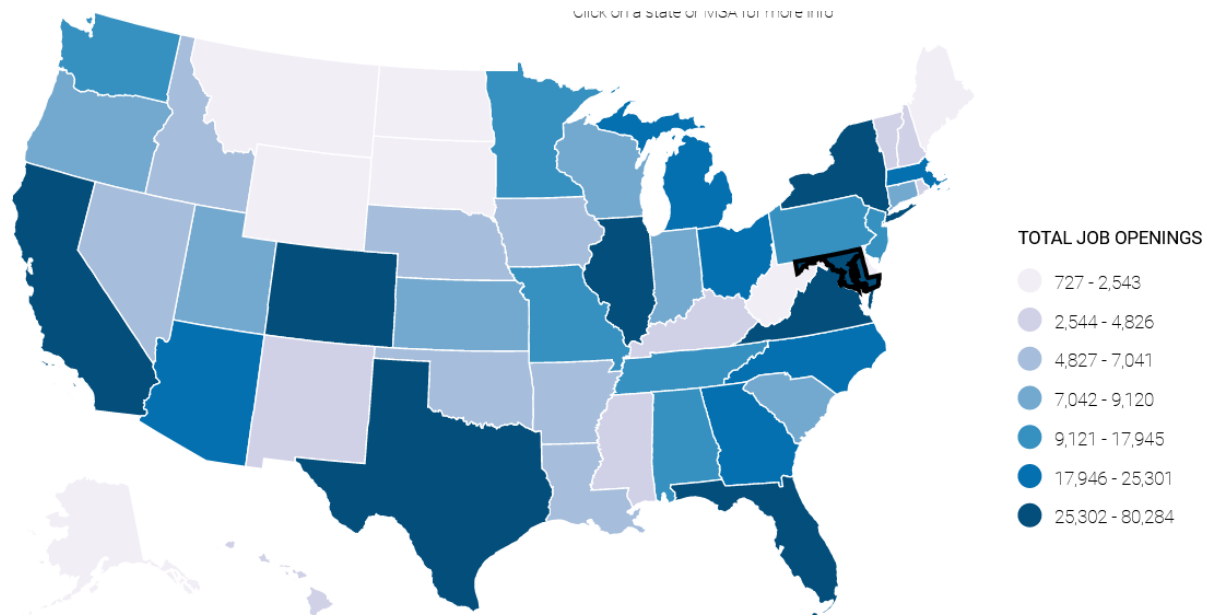
According to the U.S. Bureau of Labor Statistics the average annual salary for a cybersecurity analyst living in Maryland is \$135,920 which is the second highest in the nation. For cybersecurity professionals who are just entering the workforce the average salary in Maryland is \$82, 286 and the salary varies significantly by the location within the state of Maryland (<https://www.ziprecruiter.com/Salaries/Entry-Level-Cyber-Security-Analyst-Salary-in-Maryland>).

Figure 3: Number of open positions in Cybersecurity in 2010 and 2023



<https://www.cyberseek.org/heatmap.html>

Figure 4 : 2023 Total job openings

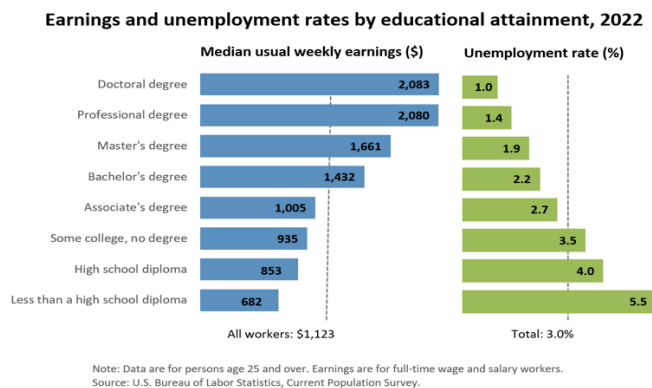


<https://www.cyberseek.org/heatmap.html>

3. Discuss and provide evidence of market surveys that clearly provide quantifiable and reliable data on the educational and training needs and the anticipated number of vacancies expected over the next 5 years.

Providing students, the opportunity to obtain a bachelor's degree increases their earning potential and is associated with a lower unemployment rate. According to recent data from 2022, unemployment rates of those with a bachelor's degree was 2.2% which is significantly lower than a 4.0% rate of those with a high school diploma. In addition, the median weekly earnings of those with high school diploma was \$853, which is \$579 less than a person with a bachelor's degree would earn (Figure 4).

Figure 5: Earnings and unemployment rates by educational attainment



The need for cybersecurity professionals is expected to continue for at least the next 10 years. According to the BLS, the number of people employed as security analyst is expected to increase by 32% in 2032 (Figure 5). Cybersecurity industry will experience the fifth highest growth in available jobs in the next 10 years. The projected rate of employment growth within the information security industry is expected to be 0.6 annually (Figure 6). Within the state of Maryland, by 2030 there will be over 100,000 available cybersecurity positions (BLS). Therefore, this demonstrates the need for establishing numerous opportunities for students to obtain training prior to entering the cybersecurity industry. Within Maryland the cybersecurity positions will be located within the Baltimore city, Baltimore County and Montgomery county areas.

Figure 6: Projected employment change

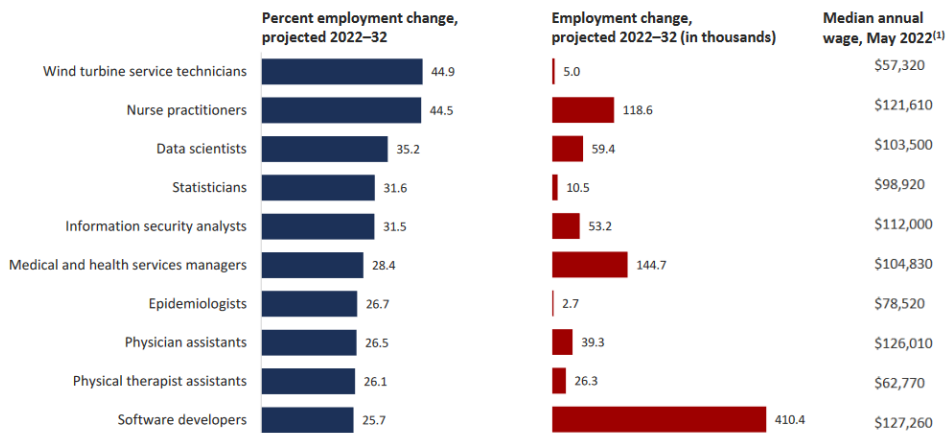
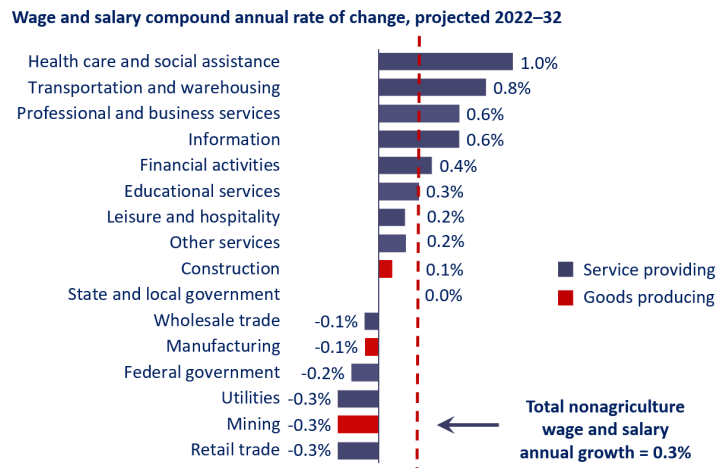


Figure 7: Projected Annual Rate of Change by Industry

Projected Annual Rate of Change in Industry Employment, 2022-32



4. Data showing the current and projected supply of prospective graduates.

The number of students enrolling in college has been steadily increasing for the past 50 years and upward trend continues. Current projections indicate that enrollment in postsecondary institutions is projected to increase by 3%, from 2017 to 2028. This increase will primarily occur among students seeking an undergraduate degree. This increase will be most evident among Hispanic students with a increase projected for Hispanic (14%) and Black/African American (8%) students and decrease (6/%) in

the number of white students who are matriculating at these institutions (nces.ed.gov). These projected increases in enrollment indicates a continued population of prospective graduates for enrollment within the cybersecurity field.

In the past twenty years the number of 4-year college graduates has increased by 90% (educationdata.org). In 2021 over two million graduates earned a bachelor's degree which is a 1.37% increase from the previous year. As the number of college graduates has increased so has the number of graduates within the STEM fields increased. In 1971, 30% of bachelor's degrees earners majored in education which decreased to 19% fifty years later. In contrast, the STEM field is one of the areas that has experienced a significant growth in the number of graduates with a bachelor's degree. While there is an increase in the number of graduates within the STEM field the increase is not sufficient to meet the demands of the cybersecurity field. This limited supply of graduates within the cybersecurity field is one of the factors why there is such a high demand for employees and the rationale for establishing this partnership with NDMU.

D. Reasonableness of Program Duplication

- 1. Identify similar programs in the State and/or the same geographical area. Discuss similarities and differences between the proposed program and others in the same degree to be awarded.**

The Cybersecurity program on the NDMU campus will be provide students with access to the resources of the typical Capitol Technology University students. Students will be taught and receive the same experiences as students in the Cybersecurity program on the Laurel campus.

- 2. Provide justification for the proposed program.**

The proposed Bachelor of Science in Cybersecurity program is strongly aligned with the University's strategic priorities and is supported by adequate resources. The proposed partnership with NDMU will provide opportunities for students to obtain a degree in Cybersecurity which is an industry that is currently in high demand but is lacking in the production of graduates.

E. Relevance to high-demand programs at Historically Black Institutions (HBIs):

- 1. Discuss the program's potential impact on the implementation or maintenance of high-demand programs at HBIs.**

The University does not anticipate any impact on the implementation or maintenance of high-demand programs at HBIs.

F. Relevance to the identity of Historically Black Institutions (HBIs):

- 1. Discuss the program's potential impact on the uniqueness and institutional identities and missions of HBIs.**

The University does not anticipate any impact on the uniqueness and institutional identities and missions of HBIs.

G. Adequacy of Curriculum Design, Program Modality, and Related Learning Outcomes (as outlined in COMAR 13B.02.03.10):

- 1. Describe how the proposed program was established, and also describe the Faculty who will oversee the program.**

The partnership with NDMU was established after discussion between the executive members of CTU and NDMU. The Chair of the Cybersecurity program will oversee the program on the NDMU campus.

- 2. Describe educational objectives and learning outcomes appropriate to the rigor, breadth, and (modality) of the program.**

Learning Objectives:

1. Be highly sought and will be recognized as having expertise in their field.
2. Demonstrate a lifelong commitment to expanding their professional expertise.
3. Demonstrate character and values by making ethical decisions throughout their professional careers.
4. Strive for the betterment of society by pursuing their vocation

Learning Outcomes:

Upon graduation, graduates will be able to:

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions
2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline
3. Communicate effectively in a variety of professional contexts
4. Recognize professional responsibilities and make informed judgments in computer practice based on legal and ethical principles
5. Function effectively as a member or leader of a team engaged in activities appropriate to the programs discipline
6. Apply security principles and practices to maintain operations in the presence of risks and threats.

- 3. Explain how the institution will:**

a) Provide for assessment of student achievement of learning outcomes in the program

Capitol Technology University will assess student achievement of the learning outcomes per the regulations specified by the University's regional accreditation organization: the Middle States Commission on Higher Education (MSCHE).

Capitol Technology University has a rigorous assessment schedule that adheres to both MSCHE and ABET guidelines. The Assistant Vice President of Assessment, Learning and Educational Effectiveness (AVPLEE) is responsible developing and implementing a rigorous and sustainable assessment process. Therefore, all assessment activities are supported and facilitated by the AVPLEE. Thus, the AVPLEE ensures that assessment activities are occurring according to schedule and that findings are utilized for continuous improvement to student learning and the program. Every five years the Cybersecurity program develops an assessment plan that identifies the program outcomes and courses that will be assessed.

Components of the five-year assessment cycle

- Completion of a curriculum map for each program
- Schedule of the program objectives/outcomes to be assessed and reassessed at least once during the cycle
- Identification of the activity (i.e., data collection or analysis) that will occur each semester
- At the end of every academic year, completion of an assessment report that summarizes findings which will be submitted to the Assistant Vice President of Assessment, Learning & Educational Effectiveness
- Assessment of the various elements of the assessment process at the end of the five-year cycle
- Completion of a review of the program

The end of the five-year assessment cycle provides data that informs the review of the program and incorporates requirements of the ABET self-study process and internal requirements.

4. Provide a list of courses with title, semester credit hours and course descriptions, along with a description of program requirements.

Program description, as it will appear in the catalog:

The Bachelor of Science in Cybersecurity prepares students to fill the skills gap in this growing field. Students gain an understanding of key cybersecurity challenges, including how to secure information and defend the information systems that store it. The program also provides a foundation in computer networking and programming. By the end of the program, students complete coursework that prepares them to pass industry certification exams, including A+, Network+, CEH, CISSP, and Security+, positioning them to graduate with industry credentials.

Admissions Requirement for Degree-Seeking Students First-Time, Full-Time Freshman

All applicants receive a comprehensive evaluation of their previous school records. Admissions decisions are based on the applicant's course preparation, high school grade point average (GPA), class rank and standardized test scores. Scholarship consideration is given based on GPA test scores, along with the admissions essay, letters of recommendation and a personal interview.

High school course preparation should include a minimum of four units of English, three units of mathematics (including plane geometry and Algebra II), two units of lab science and two units of social sciences.

Students whose GPA, course preparation and/or test scores do not meet the general admissions requirements may be further considered if they submit an admissions essay, letters of recommendation, placement tests and visit the campus for a personal interview.

The minimum GPA required for admission to Capitol Technology University is 2.2 on a 4.0 scale. The minimum SAT score is 800 composite. The minimum ACT score is 17 composite.

Full-time Transfer Students Admissions Requirements

Full-time transfer applicants who have successfully completed an associate or bachelor's degree are generally accepted into Capitol Technology University once their application file is complete. Admissions requirements for all other students are based on previous academic coursework (including high school, college, proprietary institutions, the military or appropriate work experience), with an emphasis on postsecondary achievement. Students must be in good standing at all previous institutions. Students not in good standing are subject to further review.

If applicants are not eligible to transfer credits for MA-114 or EN-101, completion of a skills assessment test may be required. Applicants who are not eligible to transfer college level math or English credits must take placement tests. Applicants with experience in computer programming who are not eligible to transfer college level credits in computer science are encouraged to take placement testing, those who choose not to take placement testing will register for CS-100. Applicants with experience in cybersecurity who are not eligible to transfer college level credits in cybersecurity are encouraged to take placement testing, those who choose not to take placement testing will register for IAE-201.

All Bachelor of Science degrees require a minimum of 27 credits at the 300-level or above. For descriptions of required courses, see courses beginning on page 211. All degree-seeking undergraduate students are required to take courses in humanities and the social sciences to broaden their understanding of professional and ethical responsibilities within a global context.

Degree Requirements:

The following is a list of courses for the **Bachelor of Science in Cybersecurity** degree. Students expecting to complete this degree must meet all prerequisites for the courses listed below.

Bachelor of Science in Cybersecurity Courses Total Credits: 120

Programming and Computer Science –33 Credits

CS-120 - Introduction to Programming Using Python

The course will cover basic concepts and elements of computer programming using Python. Topics include variables, constants, operators, expressions, statements, branching, loops, and functions. Additionally, Python specific data structures, built-in functions, library modules and working with external files will be applied in developing working code. (3-0-3)

CS-150 – Introduction to Programming Using C

This introductory course in programming will enable students to understand how computers translate basic human instructions into machine executable applications. The language of choice for this course is C. The C syntax that will be covered includes functions; variables and memory allocations including pointer notation; conditional statements and looping. Students will also learn binary to hexadecimal and decimal conversions along with basic computer architecture. Memory management, data input output and file manipulations will be among some other topics discussed and applied during this course. Prerequisite: MA-111 or MA-112 and CS-120 or placement test. Formerly titled Introduction to Programming Using C. (3-2-3)

CS-200 – Introduction to Object Oriented Programming in C++

Students learn how to program in C++ using an object oriented approach. Design of classes and objects, inheritance and polymorphism, use of pointers and data structured based projects are also covered in this course. Prerequisite CS-130 or CS-150. (2-2-3)

CS-220 - Database Management

An overview of database systems, with an emphasis on relational databases. Terminology, basic analysis and design using Entity-Relationship diagrams and relational schemas. Database implementation, queries and updates in a modern relational database management system. An overview of database administration, transactions and concurrency. Data warehouses. Projects, which are assigned as homework, are implemented in Oracle. Prerequisite: CS-120 or CS-130 or CS-150. You may take this course and CS-130 concurrently. (3-0-3)

CS-230 - Data Structures

Advance pointers and dynamic memory usage. Concepts of object-oriented design and programming. Includes classes, friend functions, templates, operator overloading, polymorphism, inheritance, exception handling, containers, iterators and the standard template library. Applications involve the use of simple data structures such as stacks, queues, linked lists and binary trees. Recursion, searching and sorting algorithms. The above concepts are implemented through a series of hands-on programming projects, all of which are completed as part of the homework requirements. Prerequisite: CS-225 or CS-200. Corequisite: MA-124. (3-0-3)

CS-250 - Introduction to Network Programming Using C

An introductory network programming course using the C programming language. Students will be provided an overview of the principles of computer networks with a detailed look at the OSI

reference model and the TCP/IP stack. The emphasis is on understanding UNIX inter-process communication and developing network programs using connectionless and connection-oriented sockets. Extensive programming assignments will include the development of client/server and peer-to-peer network applications. Prerequisites: CS-230. (2-2-3)

CS-300 - Secure Coding

This course introduces the secure coding process including designing secure code, writing code that can withstand attacks, and security testing and auditing techniques to detect secure coding weaknesses. The course focuses on the security issues a programmer faces including, but not limited to, common code security weaknesses and modern security threats. The course explores core secure coding principles, strategies, coding techniques, and tools that aid programmers in developing more resilient and robust code. Students will develop and analyze C language code that demonstrates mastery of these secure coding principles. The course will also rely on industry standards and best practices such as SEI-CERT coding standards and OWASP top 10 web application security risks. Prerequisite: CS-250 (3-0-3)

CS-418 - Operating Systems

Principles underlying computer operating systems are presented from a computer designer's perspective. Concepts explained include process concurrency, synchronization, resource management, input/output scheduling, job and process scheduling, scheduling policies, deadlock, semaphore, consumer/producer relationship, storage management (real storage management policies in a multiprogramming environment), virtual memory management (segmentation and paging), secure memory management, access control lists and kernel protection. An overview of contemporary operating systems with these principles. Students program in a high-level language. Projects are assigned as part of the homework requirements. Prerequisites: CS-150, CT-152, CS-230 and senior status. (3-0-3)

CT-152 - Introduction to UNIX

Unix file and operating system. Understanding multi-user and multitasking concepts. Editors, X-windows, Awk, email, Internet commands, shell commands and shell scripts. Projects, which provide practical experience, are completed as part of the homework requirements. Corequisite: CS-120. (3-0-3)

CT-240 - Internetworking w/ Routers/Switches

Configuring routers and switches to build multiprotocol inter-networks such as RIP, EIGRP, OSP and BGP. VLAN and VLAN trunking are also included. In addition, Point to point protocols, encapsulation and VPN will be part of the hands-on labs. Security topics that include the implementation of firewalls and mitigating threats via various authentication techniques will be part of the lab work. Prerequisites: NT-150 or professor approval. (2-2-3)

NT-150 - Computer Networking

This course is a continuation of NT-100 with major emphasis on local network equipment, network software and addressing schemes. Students build, configure, test and troubleshoot a network in the laboratory. Routers and switches are included. This material can be used as a basis for studying for CISCO's ICND1. (1-4-3)

Information Assurance—33 Credits

IAE-201 - Introduction to Information Assurance Concepts

This course covers topics related to administration of network security. Topics include a survey of encryption and authentication algorithms; threats to security; operating system security; IP security; user authentication schemes; web security; email security protocols; intrusion detections; viruses; firewalls; Virtual Private Networks; network management and security policies and procedures. Laboratory projects are assigned as part of the homework requirements. Classes are a mixture of lecture, current event discussions, and laboratory exercises. Prerequisites: MA-110 or MA-112 or MA-114 or MA-261. (3-0-3) NOTE: Students enrolled in this course incur an additional lab fee of \$100.

IAE-250 –Computer & Network Security

Building on IAE-201, this course provides learners with detailed and hands-on knowledge of computer and network security. The course emphasizes current topics such as network security, compliance and operational security, threats and vulnerabilities, application security, access control, as well as cryptography. Additionally, underlying theory and concepts are presented in order to extend learners' understanding of computer and network security. Weekly laboratory exercises are utilized to reinforce practical, real-world security techniques. Classes are a mixture of lecture, current event discussions, and laboratory exercise review and will prepare learners for the CompTIA Security+ certification. Pre-requisite: IAE-201 (3-0-3) *FORMERLY IAE-301 NOTE: Students enrolled in this course incur an additional lab fee of \$100.

IAE-260 - Secure System Administration & Operations - UNIX

This course is an overview of securing the UNIX operating system. The content will include a basic introduction of shell programming, process management, and processor management, storage management, scheduling algorithms, resource protection and system programming. The course will include programming projects focused on Information Assurance problem solving utilizing the C programming language primarily. Students are expected to be familiar with virtual machines, the UNIX command line interface (CLI) and a basic programming language. Prerequisites: IAE-201, CS-150, and CT-152. FORMERLY IAE-315 (3-0-3) NOTE: Students enrolled in this course incur an additional lab fee of \$100.

IAE-321 - Applied Wireless Network Security

This course will explore the unique challenges presented by wireless networking, including the management of dual network devices (Bluetooth, 3G, 4G, and WiFi). Students will evaluate emerging business and technical initiatives, such as bring your own device (BYOD) and securely implement mobile I.P. networks based on IPv4, IPv6 and the 3GPP. Students will learn penetration testing strategies to effectively evaluate currently implemented security controls, utilizing cutting edge tools such as BackTrack 5, Vistumbler, Wireshark, and inSIDder for network discovery and packet analysis. Additionally, students will be exposed to the site survey, network management and analysis capabilities of industry leading software such as Air Magnet, Ekahau and OmniPeek. Students are required to purchase an Alfa wireless adapter and acquire a wireless router for this class. This course prepares students for the Certified Wireless Security Professional (CWSP) Certification. Pre-requisites: IAE-250 and CT-240. (3-0-3)

IAE-325 - Secure Data Communications & Cryptography

This course follows the protocol education provided in IAE-250 with a more detailed and practical look at secure transactions and correspondence, as well as protection of data in storage. Within the confines of the ISO-OSI model, this course discusses data communication with emphasis on the security available at the layers, secure sockets layer, and both wired and wireless security topics. One-way message digests/hashes and encryption history and protocols are explored in-depth. Topics include virtual private networks, one-way hashes/message digests, digital signatures, secret-key and public key cryptography processes and algorithms.

Prerequisite: IAE-250 and CT-152. (3-0-3) NOTE: Students enrolled in this course incur an additional lab fee of \$100.

IAE-390 - Penetration Testing

This course explores the foundational concepts, methods and techniques in preparing and conducting penetration tests. Throughout the course students are introduced to various tools as well as unravel complex methods for exploiting client-side, service side and privilege escalation attacks. Most importantly students learn how to construct a final report outlining discovered vulnerabilities, make suggested recommendations to remediate and/or mitigate those vulnerabilities. Students also learn how to describe the findings wherein non-technical personnel understand the ramifications of these vulnerabilities in a business sense. This course prepares students for the EC Council Certified Ethical Hacker (CEH) certification. Prerequisites: CT-240 and IAE-260. (3-0-3) *FORMERLY IAE-410 NOTE: Students enrolled in this course incur an additional lab fee of \$100.

IAE-402 - Intro to Incident Handling & Malicious Software

This course provides a detailed understanding of incidents from attacks of malicious software. This course addresses the history and practice of coding that occurs in viruses, worms, spyware, Trojan horses, remote management back doors and root kits. Students learn preventative measures and tools and explore how to rid systems of malicious software and prevent re-infection. Recovery processes and backup methods are explored. In addition to covering basic incident handling preparation, response and recovery practices, the course goes into detail

regarding malicious software. Prerequisite: IAE-260. (3-0-3) NOTE: Students enrolled in this course incur an additional lab fee of \$100.

IAE-405 - Malware Analysis/Reverse Engineering

This course introduces students to malware research and analysis. The course will provide students an overview of malware research, intelligence gathering related to malware, and provide students basic skills required to analyze and dis-assemble malicious programs. Students will explore the tools required for analysis and reverse engineering of malicious code, learn malware defense techniques, how malware functions, and will perform live analysis and reverse engineering exercises. Prerequisite: IAE-402 (3-0-3) NOTE: Students enrolled in this course incur an additional lab fee of \$100.

IAE-406 – Digital Forensics and the Investigation Process

Students explore forensics and the investigation processes. Students explore current computer forensics tools, conduct live computer forensic analysis, conduct e-mail investigations, recovery of graphics files and data carving, and engage in report writing for high-tech investigations. This course prepares students for the AccessData Certified Examiner (ACE) and Mobile Phone Examiner Plus (MPE+) Certifications. Lab fee required. Prerequisites: IAE-260 and IAE-402. (3-0-3). NOTE: Students enrolled in this course incur an additional lab fee of \$100.

IAE-457 - Senior Design Project I

Students/teams select a project, develop an understanding of the project scope that includes research and documentation of related work, prepare a feasibility study, develop project requirements (constraints) and engineering, software, and/or security specifications, propose solutions and multiple designs, analyze proposed designs, select a final proposed design, and prepare and present a preliminary design review (PDR). Students are expected to apply proper systems engineering and project management to their work. Additional components may be required in some projects. Students/teams submit a final report at the end of the semester. Prerequisite: Senior standing. (3-0-3)

IAE-458 - Senior Design Project II

Students/teams build and test their selected designs (completed in IAE-457). Each student team delivers a tested prototype and defends its project in front of a panel of experts. Students/teams submit a final report that includes description of the design, realization, and test processes as well as test results, discussion, and conclusion. Failure to deliver a completed design and a working prototype that meets engineering, software, and/or security specifications by the end of the semester may result in failing the course. *Note: Course must be completed with a grade of “C” or higher to meet undergraduate graduation requirements. Prerequisite: IAE-457. (3-0-3)

Management—9 credits

BUS-101 – Introduction to Data Science

Fundamental coursework on the standards and practices for collecting, organizing, managing, exploring, and using data. Topics include preparation, analysis, and visualization of data and creating analysis tools for larger data sets. Co-requisite: MA-112. (3-0-3)

BUS 174 - Introduction to Business & Management

This course presents a survey of the general business and management environment. Topics include an introduction to the various forms of business, organizational structure, and their legal implications. Modern management and supervision concepts, history and development of theory and practice, the roles of managers, and the relationship between manager and employee are examined. This is a seminar course with emphasis on class discussion and collaborative learning. (3-0-3)

BUS-301 - Project Management

This course is an introduction to project management. It covers the origins, philosophy, methodology, and involves actual applications and use of tools such as MS Project. The System Development Cycle is used as a framework to discuss project management in a variety of situations. Illustrative cases are used and project leadership and team building are covered as integral aspects of good project management. Prerequisites: BUS-174, EN-101. (3-0-3)

Mathematics and Science—12 Credits

MA-112 - Intermediate Algebra

Designed for students needing mathematical skills and concepts for MA-114 and MA- 261. In this course students are introduced to equations and inequalities and learn the language of algebra and related functions, including polynomial, rational, exponential and logarithmic functions. Other topics include solving equations, inequalities and systems of linear equations; performing operations with real numbers, complex numbers and functions; constructing and analyzing graphs of functions; and using mathematical modeling to solve application problems. Prerequisite: MA-005 or placement test score. (3-0-3)

MA-124 - Discrete Mathematics

This course focuses on logic sets and sequences; algorithms, divisibility, and matrices; proof, induction, and recursion; counting methods and probability; relations, closure and equivalence relations, graphs and trees; and Boolean algebra. Prerequisite: MA-112, MA- 114 or placement test score. (3-0-3)

MA-128 - Introduction to Statistics

This course addresses probability: definitions, theorems, permutations and combinations; binomial, hypergeometric, Poisson and normal distributions; sampling distribution and central limit theorem; and estimation and hypothesis testing. Prerequisite: MA-110, MA-111 or MA-112. (3-0-3)

5. Discuss how general education requirements will be met, if applicable.

The Capitol Technology University General Education program's objectives are aligned with six distribution standards: written communication, oral communication, critical thinking, global and cultural awareness, quantitative reasoning and scientific reasoning. To achieve the general education requirements students must complete courses in the following areas:

Humanities/Social Sciences—15 credits

English Communications—6 credits

Mathematics and Science—12 credits

General Electives—12 credits

6. Identify any specialized accreditation or graduate certification requirements for this program and its students.

The program will be accredited regionally by Middle States Commission on Higher Education (MSCHE). The Cybersecurity program is accredited by the ABET Computing Accreditation Commission (CAC)

7. If contracting with another institution or non-collegiate organization, provide a copy of the written contract.

The University will be entering in partnership with Notre Dame of Maryland University (see attached)

8. Provide assurance and any appropriate evidence that the proposed program will provide students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial aid resources, and costs and payment policies.

The Bachelor of Science in Cybersecurity program will provide students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, Learning Management System, availability of academic support services and financial aid resources, and costs and payment policies.

Curriculum, course, and degree information will be available on the university website and via e-mail as well as regular mail (by request). The expectations for faculty/student interaction are available to students during virtual open house events, literature, website, etc. This information is also part of the material distributed for each course. Students receive guidance on proper behavior/interaction with their Department Chair and faculty members both in-person and online to facilitate a high-level

experience. Technology competence skills and technical equipment requirements are part of the materials distributed for each course. The technical equipment requirements are also listed on our website and provided to students in the welcome package.

The University's academic support services, financial aid resources, costs and payment policies, and Learning Management System are covered in the University Open Houses, the application process, the Welcome Aboard process, Orientation, Student Town Halls, and individual counseling.

9. Provide assurance and any appropriate evidence that advertising, recruiting, and admissions materials will clearly and accurately represent the proposed program and the services available.

The Bachelor of Science in Cybersecurity program's advertising, recruiting, and admissions materials will clearly and accurately present the program and the partnership. The content for this partnership will be consistent with information that is current displayed about the Cybersecurity program.

H. Adequacy of Articulation:

1. If applicable, discuss how the program supports articulation with programs at partner institutions. Provide all relevant articulation agreements.

The University is very active with its transfer partners throughout the state and beyond. The goal of the University is to work with partners to make the transfer as seamless as possible and to maximize the student's transfer credits as possible. There are University transfer admissions personnel to guide the student through the process. This partnership with NDMU will enhance our transfer agreements with surrounding community colleges that offer an associate degree in Cybersecurity.

I. Adequacy of Faculty Resources (as outlined in COMAR 13B.02.03.11):

1. Provide a brief narrative demonstrating the quality of the program faculty. Include a summary list of the Faculty with appointment type, terminal degree title and field, academic title/rank, status (full-time, part-time, or adjunct) and the course(s) each faculty member will teach.

Almost all of the Faculty listed below have been employed with the University for at least several years. Dr. Kellep Charles is currently the Chair of the Cybersecurity program and has worked for over 20 years at Capitol. Dr. Richard Hansen is a full-time faculty member with over 10 years of experience at Capitol. Dr. William Butler is the Director of the Center for Cyber Research and Analysis (CCRA) and has over 20 years of experience at Capitol. The University leadership is confident in the quality of the faculty and their abilities to provide a learning environment supportive of the University's goals for student success.

Instructors who will be engaged with the Cybersecurity program are:

Name	Credentials	Courses
Dr. Kellep Charles Full-time	D.Sc. Cybersecurity M.S. Telecommunications Management B.S. Computer Science CISSP	All Cybersecurity courses
Dr. Richard Hansen Full-time	Ph.D Technology M.S. Computer Science B.S. Electronic Engineering	All Cybersecurity courses
Dr. William Butler Full-time	D.Sc. Cybersecurity M.S. Telecommunications Management B.S. Computer Science	All Cybersecurity courses
Dr. Ron Hill Adjunct	Ph.D. Cybersecurity Leadership M.S. Information Security & Assurance B.S. Information Systems	All Cybersecurity courses
Dr. Chike Chike Adjunct	D.Sc. Cybersecurity M.S. Law	All Cybersecurity courses
Dr. Roderick Author Adjunct	D.Sc. Cybersecurity & Assurance M.S. Information Security & Assurance B.S. Information Systems Security & Forensics	All Cybersecurity courses
Thomas Joseph Maroney Adjunct	D.Sc. Cybersecurity M.S. Project Management B.S. Technical Management	All Cybersecurity courses
Ashanti Milow Adjunct	M.S. Information Systems B.S. Business Administration	All Cybersecurity courses
Geoffrey Weidner Adjunct	M.S. Forensic Science B.S. Electrical Engineering	All Cybersecurity courses

2. Demonstrate how the institution will provide ongoing pedagogy training for Faculty in evidence-based best practices, including training in:

a) Pedagogy that meets the needs of the students

The primary pedagogy for Faculty at Capitol Technology University is the Active Learning model. The University believes strongly in a highly interactive, thinking, and hands-on experience for students in each class to the maximum extent possible.

It was two Missouri State professors, historian Charles Bonwell and psychologist James Eison, who coined the term "active learning." In their 1991 book on the subject, *Active Learning: Creating Excitement in the Classroom*, they offered this definition of the concept: "active learning involves students in doing things and thinking about the things they are doing."

The definition, though it seems circuitous, marks a definitive pedagogical shift in college teaching and learning. Rather than think about what they are watching, hearing, or reading, students are first encouraged to be "doing" something in class, and then to apply critical thought and reflection to their own classroom work and activity. Their argument was backed up by research. Even Bligh, 20 years earlier, had pointed out that the

immediate rehearsal of new information and knowledge had a significant impact on learning.

This approach is as helpful in the sciences as it is in the arts or humanities: whether it's organic chemistry, creative writing, or behavioral economics, concepts are all best understood through repeated practice and open, social exploration. The central tenet of active learning is that practice matters, and that classroom time is better spent giving students opportunities to work with concepts over and over, in a variety of ways and with opportunities.

The central tenet of active learning — that practice and interaction matters— can be applied across disciplines for immediate feedback, so that knowledge can take hold in their own minds.

(Source: Preville, P. Active Learning: The Perfect Pedagogy for the Digital Classroom: An Essential Guide for the Modern Professor)

All Faculty receive regular periodic and recurring pedagogical training during the academic year. Those training sessions occur in a hybrid format – simultaneously live online and live on-ground in the classroom. The sessions are designed to reach all Faculty, both fulltime and adjunct, in order to ensure everyone receives the training. Additionally, the sessions are recorded for those Faculty who are unable to attend the live training session due to other professional and teaching commitments.

b) The Learning Management System

The University's Department of Online Learning and Information Technology Division supports the online program needs of Faculty and students. The Department of Online Learning and I.T. Help Desk provide 24-hour support to the faculty. Canvas is the University's online Learning Management System. When a new faculty member is assigned to teach an online course, the Department of Online Learning provides formal training for the instructor. New Faculty are assigned an experienced faculty mentor to ensure a smooth transition to the online environment as well as to ensure compliance with the institution's online teaching pedagogy. The University believes this provides the highest-level learning experience for the faculty member and, in turn, students attending online classes.

c) Evidenced-based best practices for distance education, if distance education is offered.

Faculty at Capitol Technology University receive training in Keller's ARCS Motivational Model and his associated strategies for distance education/online learning.

A model used in the online delivery of teaching and learning to increase learner motivation is Keller's ARCS motivational model. This model has been considered an important element in online education because of its implications on increased learner motivation and learning outcomes. The Keller's model consists of motivating students by maintaining and eliciting attention (A), such as virtual clinical simulations; making the content and format relevant (R), by modeling enthusiasm or relating content to future use; facilitating student confidence (C), by providing "just the right challenge"; and promoting learner satisfaction (S), by providing reinforcement and praise when appropriate.

Examples of Keller's model include increasing motivation including the arousal of curiosity of students, making the connection between learning objectives and future learning goals, autonomous thinking and learning, and fostering student satisfaction. Keller's ARCS model has been researched by various educational online programs to analyze student motivation and learning outcomes. Keller's model serves as an example and guide for instructors to motivate and increase online engagement with their students as well as research purposes.

A qualitative study by Chan Lin investigated online student learning and motivation. Discussion boards, student projects, and reflection data were collected and analyzed from a 12-week web-based course. Respondents indicated the importance of online feedback from the instructor and peer modeling of course tasks to visualize learning progress. The study revealed using Keller's ARCS strategies fosters greater student online engagement by fostering self-efficacy and a sense of accomplishment.

In a mixed-method study, assessing the use of Keller's ARCS on instructional design, the use of educational scaffolding fostered positive levels of student motivation. Relevancy, attention, confidence, and satisfaction were all common factors associated with student success in the course and course completion.

(Source: Pinchevsky-Font T, Dunbar S. Best Practices for Online Teaching and Learning in Health Care Related Programs. The Internet Journal of Allied Health Sciences and Practice. January 2015. Volume 13 Number 1.)

All Faculty receive regular periodic and recurring training on evidence-based practices for distance education/online learning during the academic year. Those training sessions occur in multiple formats: asynchronous, synchronous (i.e., live online), hybrid (i.e., simultaneously live online and live on-ground), and on-ground in the classroom. The sessions are designed to reach all Faculty, both fulltime and adjunct, to ensure all members receive the training. Additionally, the live sessions are recorded for those Faculty who are unable to attend the live training session due to other professional commitments or who are teaching classes at the training delivery time.

J. Adequacy of Library Resources (as outlined in COMAR 13B.02.03.12):

- 1. Describe the library resources available and/or the measures to be taken to ensure resources are adequate to support the proposed program. If the program is to be implemented within existing institutional resources, include a supportive statement by the President for library resources to meet the program's needs.**

Library Services: The Puente Library offers extensive services and a wide collection for Capitol Technology University students to be academically successful. Library resources are available digitally. The library also provides a mailing service for materials borrowed through the Maryland system.

The library is currently supporting the following degrees at the undergraduate level: B.S. in Astronautical Engineering, B.S. in Aviation Professional Pilot, B.S. in Computer Engineering, B.S. in Computer Engineering Technology, B.S. in Computer Science, B.S. in Construction Information Technology and Cybersecurity, B.S. in Construction Management and Critical Infrastructure, B.S. in Construction Safety, B.S. in Cyber Analytics, B.S. in Cybersecurity, B.S.

in Data Science, B.S. in Electrical Engineering, B.S. in Electrical Engineering Technology, B.S. in Engineering Technology, B.S. in Facilities Management and Critical Infrastructure, B.S. in Information Technology, B.S. in Management of Cyber and Information Technology, B.S. in Mechatronics Engineering, B.S. in Mechatronics and Robotics Engineering Technology, B.S. in Software Engineering, and B.S. in Technology and Business Management, B.S. in Unmanned and Autonomous Systems, and B.S. in Web Development.

Therefore, the library is fully prepared to support a **Bachelor of Science in Cybersecurity**. Services provided to online students include:

- "Ask the Librarian"
- Research Guides
- Tutorials
- Videos
- Online borrowing

The John G. and Beverley A. Puente Library provides access to management, decision science, and research methods materials through its 10,000-title book collection, e-books, and its 90 journal subscriptions. The library will continue to purchase new and additional materials in the management, decision science, and research methods area to maintain a strong and current collection in the subject area. Students can also access materials through the library's participation in Maryland's Digital eLibrary Consortium. This online electronic service provides access to numerous databases (Access Science, NetLibrary) that supply students with the documents they need. Available databases include ProQuest, EBSCO, ACM, Lexis Nexis, Taylor Francis, and Sage Publications.

The Puente Library can provide access to historical management and decision science materials through its membership in the Maryland Independent College and University Association (MICUA) and the American Society of Engineering Education (ASEE). Reciprocal loan agreements with fellow members of these organizations provide the library access to numerous research facilities that house and maintain archives of management and decision science documents. The proximity of the University of Maryland, College Park, and other local area research and academic libraries provide the Puente Library with quick access to these materials as well.

In addition to having access to the CTU digital library, students will also have access to the Loyola Notre Dame Library. The library provides numerous spaces for students to study along with a access to the digital catalog and other technological equipment.

K. Adequacy of Physical Facilities, Infrastructure and Instructional Equipment (as outlined in COMAR 13B.02.03.13):

- 1. Provide an assurance that the physical facilities, infrastructure, and instruction equipment are adequate to initiate the program, particularly as related to spaces for classrooms, staff and Faculty offices, and laboratories for studies in the technologies and sciences. If the program is to be implemented within existing institutional resources, include a supportive statement by the President regarding adequate equipment and facilities to meet the program's needs.**

No new facilities are required for the program. The program will utilize the NDMU facilities. The online class platform is web-based and requires no additional equipment for the institution. The current Learning Management System, Canvas, and Zoom meet the needs of the degree program.

2. Provide assurance and any appropriate evidence that the institution will ensure students enrolled in and faculty teaching in distance education will have adequate access to:

a. An institutional electronic mailing system

Capitol Technology University provides an institutional electronic mailing system to all students and Faculty. The University requires the use of the email system by all students and Faculty in all the institution's modalities of course delivery. Capitol Technology University students and Faculty are required to use the institution's email addresses (e.g., xxxxxxxx@captechu.edu) in all University matters and communications. The University uses the email capabilities in Microsoft Office 365 and Microsoft Outlook.

b. A Learning Management System that provides the necessary technological support for distance education

Capitol Technology University provides a robust Learning Management Systems (LMS) through the use of the Canvas LMS by Instructure (www.canvaslms.com). The University pairs Canvas with Zoom (zoom.us) to provide a platform for every student and faculty member to meet face-to-face in a synchronous "live" mode of communication. The University requires Canvas for every class; as a result, every course has a classroom on Canvas and Zoom. All syllabi, grades, and assignments must be entered into Canvas on a timely basis throughout the semester.

Canvas provides the world's most robust LMS. It is a 21st Century LMS; Canvas is a native cloud, Amazon Web Service hosted system. The system is adaptable, reliable, and customizable. Canvas is easy to use for students and Faculty. The system is fully mobile and has proven to be timesaving when compared to other systems. The following list provides the features of the system:

Time and Effort Savings

- **CANVAS DATA**
Canvas Data parses and aggregates more than 280 million rows of Canvas usage data generated daily.
- **CANVAS COMMONS**
Canvas Commons makes sharing a whole lot easier.
- **SPEEDGRADER ANNOTATIONS**
Preview student submissions and provide feedback all in one frame.
- **GRAPHIC ANALYTICS REPORTING ENGINE**
Canvas Analytics helps you turn rich learner data into meaningful insights to improve teaching and learning.
- **INTEGRATED MEDIA RECORDER**
Record audio and video messages within Canvas.

- **OUTCOMES**
Connect each learning outcome to a specific goal, so results are demonstrated in clearly measurable ways.
- **MOBILE ANNOTATION**
Open, annotate, and submit assignments directly within the Canvas mobile app.
- **AUTOMATED TASKS**
Course management is fast and easy with automated tasks.
- **NOTIFICATION PREFERENCES**
Receive course updates when and where you want - by email, text message, even Twitter or LinkedIn.
- **EASE OF USE**
A familiar, intuitive interface means most users already have the skills they need to navigate, learn, and use Canvas.
- **IOS AND ANDROID**
Engage students in learning anytime, anywhere from any computer or mobile device with a Web-standard browser.
- **USER-CUSTOMIZABLE NAVIGATION**
Canvas intelligently adds course navigation links as teachers create courses.
- **RSS SUPPORT**
Pull feeds from external sites into courses and push out secure feeds for all course activities.
- **DOWNLOAD AND UPLOAD FILES**
Work in Canvas or work offline—it's up to you.
- **SPEEDGRADER**
Grade assignments in half the time.

Student Engagement

- **ROBUST COURSE NOTIFICATIONS**
Receive course updates when and where you want—by email, text message, and even Facebook.
- **PROFILE**
Introduce yourself to classmates with a Canvas profile.
- **AUDIO AND VIDEO MESSAGES**
Give better feedback and help students feel more connected with audio and video messages.
- **MULTIMEDIA INTEGRATIONS**
Insert audio, video, text, images, and more at every learning contact point.
- **EMPOWER GROUPS WITH COLLABORATIVE WORKSPACES**

By using the right technologies in the right ways, Canvas makes working together easier than ever.

- **MOBILE**
Engage students in learning anytime, anywhere from iOS or Android, or any mobile device with a Web-standard browser.
- **TURN STUDENTS INTO CREATORS**
Students can create and share audio, video, and more within assignments, discussions, and collaborative workspaces.
- **WEB CONFERENCING**
Engage in synchronous online communication.
- **OPEN API**
With its open API, Canvas easily integrates with your IT ecosystem.
- **BROWSER SUPPORT**
Connect to Canvas from any Web-standard browser.
- **LTI INTEGRATIONS**
Use the tools you want with LTI integrations.
- **MODERN WEB STANDARDS**
Canvas is built using the same Web technologies that power sites like Google, Facebook, and Twitter.

Lossless Learning

- **CANVAS POLLS**
Gauge comprehension and incorporate formative assessment without the need for "clicker" devices.
- **MAGICMARKER**
Track in real-time how students are performing and demonstrating their learning.
- **QUIZ STATS**
Analyze and improve individual assessments and quiz questions.
- **LEARNING MASTERY FOR STUDENTS**
Empower students to take control of their learning.

(Source: <https://www.canvaslms.com/higher-education/features>)

Capitol Technology University has been using Canvas for over five years. Canvas has proven to be a wholly reliable LMS system that provides the necessary technological support for distance education/online learning.

L. Adequacy of Financial Resources with Documentation (as outlined in COMAR 13B.02.03.14):

1. Table 1: Resources.

TABLE 1: RESOURCES

Resource Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Reallocated Funds	\$0	\$0	\$0	\$0	\$0
2. Tuition/Fee Revenue (c + g below)	\$201,528	\$309,744	\$493,416	\$649,944	\$851,184
a. Number of F/T Students	0	0	0	0	0
b. Annual tuition/Fee rate	\$0	\$0	\$0	\$0	\$0
c. Total F/T Revenue (a x b)	\$0	\$0	\$0	\$0	\$0
d. Number of P/T Students	12	18	28	36	46
e. Credit Hour Rate	\$933	\$956	\$979	\$1,003	\$1,028
f. Annual Credit Hour	18	18	18	18	18
g. Total P/T Revenue (d x e x f)	\$201,528	\$309,744	\$493,416	\$649,944	\$851,184
3. Grants, Contracts and Other External Sources	0	0	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	\$201,528	\$309,744	\$493,416	\$649,944	\$851,184

A. Provide a narrative rationale for each of the resource categories. If resources have been or will be reallocated to support the proposed program, briefly discuss those funds.

1. Reallocated Funds

The University will not need to reallocate funds for the program.

2. Tuition and Fee Revenue

Tuition is calculated to include an annual 2.5% tuition increase. A 20% attrition rate has been calculated.

3. Grants and Contracts

There are currently no grants or contracts.

4. Other Sources

There are currently no other sources of funds.

5. Total Year

No additional explanation or comments needed.

2. Table 2: Program Expenditures.

TABLE 2: EXPENDITURES

Expenditure Category	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	\$113,468	\$155,071	\$238,421	\$325,843	\$417,486
a. #FTE	1.5	2	3	4	5
b. Total Salary	\$94,557	\$129,226	\$198,684	\$271,536	\$347,905
c. Total Benefits (20% of salaries)	\$18,911	\$25,845	\$39,737	\$54,307	\$69,581
2. Admin Staff (b + c below)	\$5,942	\$6,091	\$6,244	\$6,400	\$6,559
a. #FTE	.08	.08	.08	.08	.08
b. Total Salary	\$4,952	\$5,076	\$5,203	\$5,333	\$5,466
c. Total Benefits	\$990	\$1,015	\$1,041	\$1,067	\$1,093
3. Support Staff (b + c below)	\$59,885	\$92,076	\$125,837	\$161,230	\$198,313
a. #FTE	1.00	1.5	2	2.5	3
b. Total Salary	\$49,905	\$76,730	\$104,864	\$134,358	\$165,261
c. Total Benefits	\$9,980	\$15,346	\$20,973	\$26,872	\$33,052
4. Technical Support and Equipment	\$840	\$1,425	\$2,320	\$3,145	\$4,140
5. Library	\$0	\$0	\$0	\$0	\$0
6. New or Renovated Space	\$0	\$0	\$0	\$0	\$0
7. Other Expenses	\$5,850	\$14,210	\$25,370	\$39,330	\$56,090
TOTAL (ADD 1-7)	\$185,985	\$268,873	\$398,192	\$535,948	\$682,588

A. Provide a narrative rationale for each expenditure category. If expenditures have been or will be reallocated to support the proposed program, briefly discuss those funds.

a. Faculty

Table 2 reflects the faculty hours in total, but this does not necessarily imply that these are new hire requirements.

b. Administrative Staff

Capitol Technology University will continue with current the administrative staff through the proposed time period.

c. Support Staff

Capitol Technology University will add additional support staff to facilitate the program.

d. Equipment

Software for courses is available free to students or is freeware. Additional licenses for the LMS will be purchased by the University at the rate of \$70 per student in Year 1. The rate is estimated to increase by \$5 per year.

e. Library

Money has been allocated for additional materials to be added to the on-campus and virtual libraries to ensure the literature remains current and relevant. However, it has been determined that the current material serves the needs of this degree due to the extensive online database.

f. New or Renovated Space

No new or renovated space is required.

g. Other Expenses

Funds have been allocated for office materials, travel, professional development, course development, marketing, and additional scholarships.

h. Total Year

No additional explanation or comments needed.

M. Adequacy of Provisions for Evaluation of Program (as outlined in COMAR 13B.02.03.15):

1. Discuss procedures for evaluating courses, faculty and student learning outcomes.

The assessment process at the University consists of a series of events throughout the Academic Year. A summary report of assessment findings and how they are utilized for continuous improvement is reported to the AVPLEE at the end of every academic year.

Academic Year Assessment Events:

Fall Semester:

- At the August Faculty Retreat, the Faculty reviews any outstanding student learning challenges that have not been adequately addressed. The issues are brought to the Academic Dean for review and development of implementation plans.
- Faculty submit performance plans consistent with the mission and goals of the University and department. The documents are reviewed and approved by the Academic Dean.
- Department Chairs and Academic Dean review the Graduating Student Survey data.
- Department Chairs and Academic Dean review student internship evaluations.
- Department Chairs and Academic Dean review grade distribution reports from the spring and summer semesters.
- Department Chairs and Academic Dean review student course evaluations from the Summer Semester.
- Departments conduct Industrial Advisory Board meetings to review academic curriculum recommendations. The Advisory Board meets to begin curriculum review or address special issues that may arise related to the curriculum. Based on an analysis and evaluation of the results, the Academic Dean, Faculty, and the advisory boards will develop the most effective strategy to move the changes forward.

- Department Chairs conduct interviews with potential employers at our Career Fair.

Spring Semester:

- Faculty Performance Plans are reviewed with Faculty to identify issues of divergence and to adjust the plan as needed.
- Department Chairs and Academic Dean review grade distribution reports from the Fall Semester.
- Department Chairs and Academic Dean review the Graduating Student Survey data.
- Department Chairs and Academic Dean review student course evaluations from the Fall Semester and the Spring Semester (in May before the Summer Semester begins).
- Department Chairs and Academic Dean meet to review the content of the graduating student, alumni, and course surveys to ensure the surveys continue to meet the University's assessment needs.
- At the Annual Faculty Summit in May, the faculty review and discuss student learning challenges from the past academic year and provide recommendations to the Academic Dean. The results also lead to implementation plans for improvement.
- Department Chairs conduct interviews with potential employers at our Career Fair.
- Departments conduct Industrial Advisory Board meetings to review academic curriculum recommendations.

In addition to these summative assessments, students have an opportunity to provide feedback to Faculty on their experiences in the course. The course evaluation is distributed at the end of semester and the results are available to Faculty after grades have been submitted. Faculty are encouraged to review the results from the course evaluation to garner areas of continuous improvement.

The Faculty Senate meets monthly from August through April. The Faculty Senate addresses issues that impact student outcomes as these issues emerge. The leadership of the Faculty Senate then provides a report on the matter to the Academic Dean. The report may include a recommendation or a request to move forward with a committee to examine the issue further. In most cases, the changes only require the Academic Dean to inform the Vice President of Academic Affairs and University President and provide a report that includes a justification and the impact of changes as well as a strategic plan. Significant changes typically require the approval of the Executive Council.

- 2. Explain how the institution will evaluate the proposed program's educational effectiveness, including assessments of student learning outcomes, student retention, student and Faculty satisfaction, and cost-effectiveness.**

Student Learning Outcomes:

Student learning outcomes for the Cybersecurity program will be assessed based on the five-year assessment schedule that was discussed in section G. Each student learning outcome will be assessed and reassessed at least once during the five-year period. The findings from the assessment will be utilized for continuous improvement at the course and program levels.

Student Retention:

The University maintains a comprehensive student retention program under the Vice President for Student Engagement. The program assesses student retention at all levels, including the individual course, major, and degree. During the semester and term, the University's Drop-Out Detective capability, within its Learning Management System (i.e., Canvas), provides an early alert at the course level to potential issues related to retention. Within the Office of Student Life, Academic Advisors monitor Drop-Out Detective and contact students who appear to have problems with their academic performance. The Academic Advisors work with each student to create a plan to remove any barriers to success. The Academic Advisors also work with the course instructors as needed to gain additional insight that may help correct the situation.

Each student also meets with their Academic Advisor each semester to evaluate their progress toward degree completion. An updated plan of action is developed for each student for their next semester's registration and each following semester through degree completion.

The Vice President for Student Engagement also meets regularly with the Vice President of Academic Affairs and Academic Dean to review student retention within each degree program and address any issues that appear to be impediments to degree completion.

Student and Faculty Satisfaction:

Evaluations and assessment of Student and Faculty satisfaction occur every semester. Faculty members are evaluated every semester by students enrolled in their courses. Students are required to complete a course evaluation online within a specified time frame at the end of the semester for every enrolled course. Every faculty member is also required to review each of their courses after each semester; the goal is to ensure up-to-date content, effective and efficient methods of delivery, and appropriate outcomes.

The Department Chairs and Academic Dean review the student evaluations for every course offered at the University. The Department Chairs and Academic Dean also review faculty satisfaction every semester. If changes are needed at the course level, the changes are developed and implemented by the Faculty upon approval of the Department Chairs and Academic Dean. If changes are required at the faculty level, the Department Chairs will make the changes. At the end of the following semester, appropriate stakeholders analyze the results of a follow-on evaluation for the effectiveness of the changes. This cycle is an ongoing process.

Cost Effectiveness:

Based on the year-long inputs, evaluations, and reviews described in Section M.1, the Department Chairs and Academic Dean prepare the proposed academic budget for each program for the upcoming year. Budget increases are tied to increasing student learning and performance as well as critical strategic initiatives.

The Vice President of Finance and Administration also monitors each academic program throughout every semester and term for its cost-effectiveness. Additionally, the revenue and costs of every University program are reviewed annually by the Executive Council and Board of Trustees before approving the next year's budget.

N. Consistency with the State's Minority Student Achievement goals (as outlined in COMAR 13B.02.03.05 and the State Plan for Post-Secondary Education):

- 1. Discuss how the proposed program addresses minority student access & success, and the institution's cultural diversity goals and initiatives.**

Capitol Technology University is a majority-minority school. Our programs attract a diverse set of students who are multiethnic and multicultural. The University actively recruits minority populations for all undergraduate and graduate-level degrees. Special attention is also provided to recruit females into the STEM and multidisciplinary programs at all degree levels – undergraduate, master's, and doctoral. The University will use the same approach for this partnership with NDMU.

O. Relationship to Low Productivity Programs Identified by the Commission:

- 1. If the proposed program is directly related to an identified low productivity program, discuss how the fiscal resources (including Faculty, administration, library resources, and general operating expenses) may be redistributed to this program.**

This program is not associated with a low productivity program identified by the Commission.

P. Adequacy of Distance Education Programs (as outlined in COMAR 13B.02.03.22)

- 1. Provide affirmation and any appropriate evidence that the institution is eligible to provide Distance Education.**

Capitol Technology University is fully eligible to provide distance education. The University has a long history of providing high-quality distance education. The University is accredited regionally by the Middle States Commission on Higher Education (MSCHE) and through three specialized accrediting organizations: Accreditation Board for Engineering and Technology (ABET), NSA, and DHS. All accrediting organizations have reviewed the University's distance education program as part of their accreditation process. Capitol Technology University is fully accredited by MSCHE, ABET, NSA, and DHS. The University is in good standing with all its accrediting bodies.

- 2. Provide assurance and any appropriate evidence that the institution complies with the C-RAC guidelines, particularly as it relates to the proposed program.**

Capitol Technology University has a long history of providing high-quality distance education/online learning that complies with the Council of Regional Accrediting Commissions (C-RAC) Interregional Guidelines for the Evaluation of Distance Education. The University will also continue to abide by the C-RAC guidelines with the proposed program.

a. Council of Regional Accrediting Commissions (C-RAC) Interregional Guidelines for the Evaluation of Distance Education.

- 1. Online learning is appropriate to the institution's mission and purposes.**

Online learning is consistent with the institution's mission, purpose, and history. Please refer to Section A of this proposal.

- 2. The institution's plans for developing, sustaining, and, if appropriate, expanding online learning offerings are integrated into its regular planning and evaluation**

processes.

All programs at the University – online, hybrid, and on-ground – are subject to the same regular planning, assessment, and evaluation processes. Please see Section M of this proposal for the detailed process.

3. Online learning is incorporated into the institution's systems of governance and academic oversight.

All programs at the University – online, hybrid, and on-ground – are subject to the same regular planning, assessment, and evaluation processes. Please see Section M of this proposal for the detailed process.

4. Curricula for the institution's online learning offerings are coherent, cohesive, and comparable in academic rigor to programs offered in traditional instructional formats.

Online programs/courses meet the same accreditation standards, goals, objectives, and outcomes as traditional instruction at the University. The online course development process incorporated the Quality Matters research-based set of standards for quality online course design to ensure academic rigor of the online course is comparable to the traditionally offered course. The University Academic Dean, chairs, and faculty review curriculum annually. Courses are reviewed at the end of each term of course delivery. This process applies to online and traditional classes. In addition, advisory boards are engaged in the monitoring of course quality to ensure quality standards are met regardless of the delivery platform.

5. The institution evaluates the effectiveness of its online learning offerings, including the extent to which the online learning goals are achieved, and uses the results of its evaluations to enhance the attainment of the goals.

Online programs/courses meet the same accreditation standards, goals, objectives, and outcomes as traditional classroom delivery. The University selects the learning platforms to ensure the high standards of the technical elements of each course. The Academic Dean monitor any course conversion from in-class to online to ensure the online course is academically equivalent to the traditionally offered course and that the technology is appropriate to support the expected rigor and breadth of the course.

6. Faculty responsible for delivering the online learning curricula and evaluating the students' success in achieving the online learning goals are appropriately qualified and effectively supported.

The Cybersecurity department, where this degree will be housed is staffed by a qualified University Academic Dean, Dr. Kellep Charles. Other appropriately credentialed Faculty with multi-disciplinary level skills will be part of the delivery process.

The evaluation of the courses in the program will be done using the same processes as all other programs at the University (Please see Section M). All Capitol Technology University faculty teach in the traditional classroom environment and online. (Please see faculty qualifications in Section I of this document).

7. The institution provides effective student and academic services to support students enrolled in online learning offerings.

Students can receive assistance in using online learning technology via several avenues. Student aides are available to meet with students and provide tutoring support in both subject matter and use of the technology. Tutors are available in live real-time sessions using Zoom or other agreed-upon tools. Pre-recorded online tutorials are also available.

In addition to faculty support, on-ground and online tutoring services are available to students in a one-on-one environment.

Laboratories (on ground and virtual) are available for use by all students. Faculty and highly-qualified tutors staff the laboratories and provide academic support.

Library services and resources are appropriate and adequate. Please refer to Section J of this document and the attached letter from the University President. The library adequately supports the students learning needs.

8. The institution provides sufficient resources to support and, if appropriate, expand its online learning offerings.

The University has made the financial commitment to the program (please refer to Section L). The University has a proven record of accomplishment in supporting degree completion.

9. The institution assures the integrity of its online offerings.

Current Faculty serve on internal advisory boards that examine possible for program changes, including course and program development. All Faculty are selected on domain expertise and program-related teaching experience.

When new Faculty or outside consults are necessary for the design of courses offered, the University's Human Resource Department initiates a rigorous search and screening process to identify appropriate Faculty to design and teach online courses. Again, all Faculty are selected on domain expertise and program-related teaching experience.

The University online platforms offer several avenues to support instructors engaged in online learning. The Director of Online Learning Division is highly skilled and trained in faculty development. Several seminars and online tutorials are available to the Faculty every year. Mentors are assigned to new Faculty. Best practice sharing is facilitated through the Academic Dean, Department Chairs, and formal meetings.

The assessment for online learning classes/students is the same as for all academic programs at the University. Faculty provide required data on student achievement. The Learning Management System includes data on student achievement. Proof of these assessments is available during the class and following class completion to the Academic Dean and Department Chairs. On an annual basis, the information is reported to the University's accreditation authorities such as MSCHE and NSA/DHS.